WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

AN EFFECTIVE PRIVACY PRESERVING BLOCKCHAIN ASSISTED SECURITY PROTOCOL

Thrisha Reddy** *, *Chandana GS, ***Hruthika SN, **

*Computer Engineering AI & ML , Presidency University, Yelahanka,Bangalore, India
THRISHAREDDY.20211CEI0166@presidencyuniversity.in
** Computer Engineering AI & ML , Presidency University, Yelahanka,Bangalore, India
Email: CHANDANA.20211CEI0141@presidencyuniversity.in
*** Computer Engineering AI & ML , Presidency University, Yelahanka,Bangalore, India HRUTHIKA.20211CEI0157@presidencyuniversity.in
******Associate Professor, Department of Computer Science and Engineering, Presidency University,Yelahanka, Bangalore, India

ABSTRACT :

The rapid adoption of Digital Twin (DT) technology in cloud-assisted environments has introduced critical security and privacy challenges, particularly in secure data sharing, integrity verification, and user privacy preservation. Existing authentication mechanisms often lack the essential features of user anonymity, mutual authentication, and robust resistance to identity and password guessing attacks, leaving DT systems vulnerable to various security threats. To address these challenges, this paper proposes an effective privacy-preserving blockchain-assisted security protocol tailored for cloud-based DT environments. The protocol integrates blockchain technology for transparent and immutable data integrity verification and employs elliptic curve cryptography (ECC) to enable lightweight, certificate-less authentication. By leveraging the decentralized nature of blockchain and the computational efficiency of ECC, the proposed solution ensures secure communication, robust authentication, and privacy preservation while mitigating risks such as impersonation and data tampering. Comprehensive security analysis and performance evaluation demonstrate the protocol's resilience to a wide range of attacks and its feasibility for deployment in resource-constrained cloud-assisted DT scenarios.

Key Words — Block chain technology, Digital twin,ECC,Secure communication.

INTRODUCTION :

Background

This project aims to design and implement a privacy-preserving authentication protocol for Digital Twin (DT) environments, leveraging the security of blockchain technology and the efficiency of certificateless cryptography. Digital Twins are real-time virtual replicas of physical systems used in various industries like manufacturing, healthcare, and IoT. However, securely sharing and verifying the data exchanged between users, devices, and cloud services remains a significant challenge.

To address these challenges, this project proposes a secure framework that uses blockchain to store hash values of the data generated by DTs. The blockchain ensures that the data remains tamper-proof and verifiable by all participants in the network. The certificateless cryptography scheme is employed to solve issues related to traditional cryptosystems, such as complex certificate management and key escrow problems. This ensures that the authentication process is efficient ad resistant to various security attacks, such as impersonation and password guessing.

The proposed system combines Elliptic Curve Cryptography (ECC) with a blockchain-assisted infrastructure, enabling fast and secure communication between legitimate users without relying on traditional certificate authorities. The use of ECC enhances computational efficiency, making it suitable for the resource-constrained environment of IoT devices that support Digital Twins.

Approach

This research proposes a privacy-preserving blockchain-assisted security protocol for cloud-assisted DT environments to address these challenges. The proposed framework leverages blockchain technology to ensure tamper-proof, transparent, and decentralized verification of data integrity. Blockchain stores hash values of DT data and logs transaction records, enabling secure verification without reliance on centralized authorities. To resolve authentication limitations, a certificateless cryptographic approach is employed, eliminating the need for certificate management while mitigating the key escrow issue. Additionally, Elliptic Curve Cryptography (ECC) is integrated to ensure lightweight, efficient, and scalable authentication suitable for resource-constrained environments like IoT-enabled DT systems.

By combining blockchain and certificateless cryptography, the proposed solution ensures robust resistance to impersonation, password guessing, and replay attacks, while supporting mutual authentication and session key security. This innovative approach offers a scalable and efficient framework for secure interactions in complex DT ecosystems, addressing both current and future security challenges in the evolving landscape of cloud-assisted DT environments.

The system must integrate blockchain technology to record and verify data integrity, storing hash values of DT data and maintaining a tamper-proof log of transactions. It should also facilitate secure communication among users by utilizing Elliptic Curve Cryptography (ECC) to ensure that authentication processes are both efficient and resistant to common security threats such as impersonation and password guessing.

Additionally, the system must provide mechanisms for users to verify the integrity of received data through blockchain, ensuring that data tampering is detectable. The solution must support mutual authentication to verify both users and devices, and session key management to maintain secure communication sessions.

Problem Statement

The implementation of Digital Twin (DT) technology in cloud-assisted environments faces significant challenges related to secure data sharing, integrity verification, and privacy preservation. As data generated from physical assets is transmitted to cloud servers for simulation and analysis, the risk of sensitive information being intercepted or tampered with by adversaries becomes a major concern. Existing authentication mechanisms often fail to provide essential security features such as user anonymity, mutual authentication, and protection against identity and password guessing attacks. Additionally, traditional cryptographic systems suffer from complex certificate management and key escrow issues, making them unsuitable for secure DT environments. To address these challenges, there is a need for a robust and efficient authentication protocol that ensures secure communication, data integrity, and privacy preservation in cloud-assisted DT environments. The solution must withstand various security threats, including impersonation attacks, and facilitate secure data sharing between data owners, users, and cloud servers. This problem can be resolved by leveraging blockchain technology to verify data integrity through hash values and elliptic curve cryptography (ECC) for efficient, certificate-less authentication.

LITERATURE SURVEY :

I. Historical Development

• The concept of Digital Twin (DT) was first introduced by Grieves and Vickers in 2002 and later formally adopted by NASA in 2010 for space exploration projects. Initially developed to enhance Product Lifecycle Management (PLM), DTs have since evolved to become a critical component of Industry 4.0 and the Industrial Internet of Things (IIoT). By creating real-time digital replicas of physical systems, DTs enable predictive maintenance, real-time simulation, and optimization across domains such as healthcare, manufacturing, smart cities, and autonomous vehicles In parallel, the rise of *blockchain technology* began reshaping data management and security. Introduced in 2008 by Satoshi Nakamoto as the backbone of Bitcoin, blockchain's ability to provide tamper-proof, decentralized, and transparent data storage made it appealing beyond cryptocurrencies. Its applications quickly extended to sectors like supply chain management, finance, and IoT. As the IoT ecosystem expanded, researchers recognized blockchain's potential for enhancing data integrity and trustworthiness in distributed environments.

• **Blockchain for Data Security and Privacy in IoT and Cloud Computing** Zheng et al. provided a comprehensive overview of blockchain technology, identifying its applications in securing IoT and cloud environments. Blockchain ensures data integrity and immutability by maintaining tamper-proof transaction logs. However, this study also highlights scalability challenges, particularly in large-scale IoT ecosystems. The authors suggest that while blockchain strengthens data security, it is not designed to handle the privacy of user interactions or sensitive data, leaving room for enhanced privacy-preserving solutions.

•**Privacy-Preserving Authentication Protocols** Liu et al. explored certificateless cryptography as a solution to the key escrow problem in traditional public key infrastructure (PKI) and identity-based cryptography (IBC). Their proposed two-party authenticated key agreement protocol enhances computational efficiency and eliminates the need for certificate management. However, while the protocol resolves some privacy concerns, it lacks resilience against certain sophisticated attacks, such as impersonation and password guessing, that are common in decentralized cloud environments.

II. Technological Components

• **Blockchain Technology** Blockchain forms the backbone of the proposed system, enabling secure and tamper-proof data storage and verification. Key features of blockchain that make it integral to DT environments include:

- *Decentralization*: Blockchain eliminates reliance on a single centralized authority by distributing data across a peer-to-peer network, ensuring transparency and trust in data handling.
- **Data Immutability:** Transactions in the blockchain are verified using consensus mechanisms (e.g., Proof of Work, Proof of Stake), ensuring that once data is recorded, it cannot be altered. This is critical for maintaining the integrity of DT data.
- **Merkle Trees:** Blockchain uses Merkle trees to efficiently store and verify the hash values of DT data, enabling users to confirm the authenticity of received data without accessing the full ledger.

• **Certificateless Cryptography** Traditional cryptographic systems like Public Key Infrastructure (PKI) and Identity-Based Cryptography (IBC) face challenges in certificate management and key escrow, making them unsuitable for resource-constrained DT environments. Certificateless cryptography eliminates these issues by dividing the responsibility for key generation between a trusted third party (Key Generation Center, or KGC) and the user.

Elliptic Curve Cryptography (ECC)**:** A lightweight cryptographic algorithm that offers the same level of security as traditional methods like RSA but with significantly smaller key sizes. This makes ECC highly efficient and suitable for DT environments that include IoT devices with limited

computational resources.

- **Scalability:** ECC's computational efficiency allows it to support large-scale DT ecosystems without compromising system performance.

• **Three-Factor Authentication** Sensors such as The proposed system enhances authentication by employing a three-factor approach, which combines:

- *Knowledge Factor*: A user-generated password or PIN.
- *Possession Factor*: A smart card or device associated with the user.
- *Inherence Factor*: A biometric identifier (e.g., fingerprint or facial recognition).

• *Decentralized Data Verification* Decentralized verification mechanisms are employed to ensure trustworthiness without relying on a central authority:

- **Blockchain Nodes:** These nodes independently verify transactions and data integrity, ensuring a distributed consensus.
- *Cross-Chain Interoperability***:** The proposed system can interact with multiple blockchains, enabling data sharing across different systems while maintaining security and privacy. accommodate growing data volumes as supply chains expand.

III. Challenges and Limitations

The implementation of a privacy-preserving blockchain-assisted security protocol in Digital Twin (DT) environments involves addressing numerous technical, operational, and scalability challenges. While significant advancements have been made, several limitations persist that must be addressed for widespread adoption and effectiveness.

• **Data Security and Privacy Risks:** Digital Twin environments generate and transmit vast amounts of sensitive data to cloud servers for simulation and analysis. Ensuring the confidentiality, integrity, and privacy of this data is a significant challenge:

- *Data Tampering*: Adversaries can intercept or alter data during transmission, compromising its integrity.
- **Unauthorized Access:** Without robust access controls, sensitive data may be accessed by unauthorized users, leading to potential misuse.

*Limitations of Traditional Cryptographic Systems***:** Traditional cryptographic systems, such as Public Key Infrastructure (PKI) and Identity-Based Cryptography (IBC), are not well-suited for DT environments due to the following:

- *Certificate Management Overhead***:** PKI relies on certificates that require complex management, including issuance, renewal, and revocation.
- *Scalability Issues*: The computational overhead of traditional systems limits their applicability in resource-constrained IoT devices supporting DTs.

IV. Case Studies and Real-World Implementations

• **Real time implementation** The proposed privacy-preserving blockchain-assisted security protocol for Digital Twin (DT) environments integrates blockchain technology, certificateless cryptography, and elliptic curve cryptography (ECC) to address security and privacy challenges in cloud-assisted DT ecosystems. Its implementation can be effectively applied across various domains, such as healthcare, manufacturing, and smart cities.

Implementation scenario A healthcare system can implement the proposed framework for patient monitoring using IoT devices. Patient data is transmitted to cloud servers for analysis and stored on the blockchain for verification. Certificateless cryptography ensures secure authentication of healthcare providers accessing the data, and ECC ensures efficient encryption.

• **Case Study: Healthcare IoT System** One of the most impactful applications of the proposed framework is in the healthcare sector, where privacy and data integrity are paramount. A hospital integrates IoT devices and Digital Twins for patient monitoring. These DTs simulate a patient's real-time health data, such as heart rate, oxygen levels, and blood pressure, to assist doctors in diagnosing and treating patients remotely.

•*Authentication and Access Control*: Certificateless cryptography secures authentication for doctors, nurses, and other authorized personnel, preventing unauthorized access to patient data. transportation strategies, reducing costs and environmental impact. The protocol guarantees user anonymity and unlinkability, ensuring that patient identities are protected even during data sharing.

Simplified key management reduces the overhead associated with traditional cryptographic systems. addressing challenges and leveragingadvancements in IoT, track-and-trace systems have revolutionized supply chain management, setting the stage for more resilient and efficient logistics networks.

I. Proposed System :

Certificateless cryptosystems provide a robust solution to the challenges associated with traditional cryptographic systems, such as certificate management in Public Key Infrastructure (PKI) and key escrow issues in Identity-Based Cryptography (IBC).

1. To overcome these limitations, certificateless cryptography eliminates the need for certificates while also mitigating the key escrow issue. In this paradigm, a trusted third party, called the Key Generation Center (KGC), generates only a partial private key for each user. The responsibility for generating the complete private key lies with the user, who combines the partial private key with their own secret information. This dual process significantly reduces the risk of key compromise, as the KGC does not have access to the user's full private key. This enhances security while simplifying key management.

2. By incorporating blockchain, data integrity, transparency, and immutability are ensured, while the certificateless cryptosystem enables secure, efficient, and scalable user authentication. Blockchain also adds an additional layer of security by enabling decentralized verification of transactions and data, further ensuring the integrity and privacy of communications in DT environments. This combination of certificateless cryptography and blockchain results in a highly secure, efficient, and privacy-preserving authentication protocol for modern decentralized systems.

3. A malicious adversary can replay, insert, eavesdrop, modify and delete transmitted messages sent through an open channel.

- An adversary can use the ‘‘power-analysis attacks to extract the secret credentials stored on a stolen user’s smart card or mobile device’’.
- During the registration phase, the adversary can capture or tamper smart device. As a result, an adversary is able to obtain the secret credentials from the device’s memory and can attempt various other security attacks.
- Adversary could be a registered user or a malicious insider or vice-versa.
- Adversary can simultaneously perform offline identity and password guessing attacks. As a result, the adversary is able to simultaneously determine the genuine user’s identity and password.

4. An important outcome of preliminary investigation is the determination that the system request is feasible. This is possible only if it is feasible within limited resource and time.

Operational Feasibility deals with the study of prospects of the system to be developed. This system operationally eliminates all the tensions of the Admin and helps him in effectively tracking the project progress. This kind of automation will surely reduce the time and energy, which previously consumed in manual work. Based on the study, the system is proved to be operationally feasible.

Economic Feasibility Cost-benefit is an assessment of the economic justification for a computer based project. As hardware was installed from the beginning & for lots of purposes thus the cost on project of hardware is low. Since the system is a network based, any number of employees connected to the LAN within that organization can use this tool from at anytime. The Virtual Private Network is to be developed using the existing resources of the organization. So the project is economically feasible.

Technical Feasibility According to Roger S. Pressman, Technical Feasibility is the assessment of the technical resources of the organization. The organization needs IBM compatible machines with a graphical web browser connected to the Internet and Intranet. The system is developed for platform Independent environment. Java Server Pages, JavaScript, HTML, SQL server and WebLogic

Server are used to develop the system. The technical feasibility has been carried out. The system is technically feasible for development and can be developed with the existing facility.

System Architecture

The system architecture described in the report revolves around integrating Digital Twin (DT) environments, blockchain technology, and certificateless cryptography to ensure secure, efficient, and privacy-preserving operations. Below is a detailed breakdown of the architecture:

Key Components and Their Functions:

- **Data Owner**: The data owner is responsible for uploading datasets to the system and managing their integrity and confidentiality.
- **Data User**: Data users access the datasets provided by data owners. They perform functions such as requesting specific data attributes, retrieving data details, and verifying data through blockchain.
- **Blockchain Module**: Acts as a decentralized ledger for storing hash values of the data, ensuring tamper-proof and verifiable transactions.It enables users to validate data integrity using Merkle trees and supports the creation of new blockchain blocks. Maintains an immutable log of shared data among users, servers, and data owners.
- **Cloud Server**: Serves as the primary storage for datasets and intermediary for data access. Functions include storing data, processing user requests, and facilitating authorization mechanisms.
- **Key Generation Center (KGC)**: Part of the certificateless cryptographic system. Generates partial private keys for users, while the complete private key is created by combining the partial key with user-specific secrets, ensuring that the KGC cannot compromise user data.

Data Flow and Functional Process:

Data Upload and Hash Generation: Data owners upload datasets to the cloud server. Hash values for these datasets are generated and stored on the blockchain for integrity verification.

User Authentication and Key Management: The system employs a three-factor privacy-preserving authentication protocol using certificateless cryptography. This includes:

- **Mutual Authentication**: Ensures both the user and the server verify each other.
- **Elliptic Curve Cryptography (ECC)**: Provides lightweight, secure cryptographic operations suitable for IoT and resource-constrained environments.

Data Request and Verification: Data users request specific attributes or datasets via the cloud server. The blockchain verifies the integrity of the requested data using its stored hash values.

Decentralized Security Enforcement: The blockchain ensures that any tampering with data or unauthorized access is detectable. Data logs are immutably stored, providing a transparent audit trail.

Advantages of the Architecture

1. *Scalability*:
    - The combination of blockchain and cloud computing supports large-scale operations, with decentralized data verification ensuring performance consistency.
2. *Security Features*:
    - Resistance to attacks like impersonation, identity guessing, and data tampering.
    - Privacy-preserving authentication ensures anonymity and confidentiality.
3. *Efficiency*:
    - ECC ensures computational and storage efficiency, which is particularly beneficial for IoT and DT applications.

High-Level Design

The high-level design includes four primary layers:

1. *User Layer*:
    - Represents interactions between data owners, data users, and the system.
    - Facilitates authentication and data requests.
2. *Blockchain Layer*:
    - Handles data integrity checks, decentralized transaction verification, and immutable logging.
3. *Cloud Storage Layer*:
    - Manages datasets and metadata storage, acting as the primary repository for data.

Authentication and Security Layer: Integrates certificateless cryptography and ECC for secure communication and key management. Ensures that unauthorized access is detected and mitigated.

MODULE DESCRIPTION :

Data Owner

In this module, he logs in by using his/her user name and password. After Login then the data owner performs the following operations such as Upload Datasets, View All Uploaded Datasets, View All User Requests.

Data User

In this module, he logs in by using his/her user name and password. After Login the user will do some operations such as Request Data Attributes, Find Data Details, Find Data Details By Block chain.

Block chain

In this module, the Block chain can do following operations such as Login, Create Block chain and View All Datasets By Location Block chain.

Cloud Server

The Cloud server as a server to provide data storage service and can also do the following operations such as View Data Users and Authorization, View Data Owner and Authorization, View All Datasets, View All Data Requests, View Location Data Results, View Impersonation Attacks Results.

Data Collection Process

The data collection process involves acquiring data from physical assets (e.g., sensors, IoT devices) and transforming it into a virtual format for simulation and analysis within the Digital Twin environment. The key aspects of this process include:

Data Generation:

Data is generated from physical assets in real-time.

Data Integrity and Verification:

The data is hashed, and the hash values are stored in the blockchain to ensure immutability and verifiability.

Data Sharing:

The collected data is securely transmitted to the cloud server and made accessible to authorized users.

1. **Components Involved in Data Collection:**

Physical Assets and IoT Devices:

- Act as the primary sources of data. Include sensors, wearable devices, machinery, and other equipment capable of generating real-time operational data. Example: In a healthcare DT environment, sensors in wearable devices collect health metrics such as heart rate and temperature.

Data Owner:

- Manages the initial data upload to the system. Ensures that the data collected is accurate and ready for analysis in the Digital Twin environment.

Cloud Server:

- Serves as a central repository for collected data.
- Provides the computational power for simulations and facilitates data access for users.

Blockchain:

- Stores the hash values of collected data to ensure its integrity.
- Allows verification of data authenticity without exposing the actual data content.

Data Acquisition:

- Physical assets equipped with sensors collect data and transmit it to a processing node or edge device.
- The collected data may include parameters like temperature, pressure, performance metrics, and environmental conditions.

Preprocessing:

- Data is cleaned and transformed to ensure quality and relevance.
- For example, redundant or corrupted data points are filtered out to maintain system efficiency.

Hash Generation:

- A hash value is generated for the collected data using cryptographic algorithms (e.g., SHA-256).
- This ensures a unique and immutable representation of the data for blockchain storage.

Data Upload to Cloud:

- The processed data is securely transmitted to the cloud server, where it is stored and made accessible for further processing.
- The cloud also provides simulation capabilities for the Digital Twin environment.

Blockchain Integration:

- The hash value of the data is stored in the blockchain, creating an immutable and verifiable record.
- This ensures that any alteration to the original data can be detected by comparing the hash values.

Access Control and Distribution:

- Users can request specific data attributes via the system interface.
- The blockchain validates the integrity of the requested data before it is shared with users.

Challenges and Considerations :

1. *Real-Time Processing*:
   - Collecting and verifying data in real time can be computationally intensive,particularly in resource-constrained environments.
2. *Scalability*:
   - The system must handle large volumes of data generated by numerous IoT devices in a scalable manner.
3. *Privacy Preservation*:
   - Ensuring that sensitive data remains confidential while allowing authorized access for analysis and verification.
4. *Data Synchronization*:
   - Maintaining consistency and accuracy across distributed nodes in the system.

OUTCOMES.

I. Strengthened Data Security

1. *Immutability and Data Integrity*:
   - The integration of blockchain ensures that all data transactions and hash values are stored in an immutable ledger.
   - Users can verify the integrity of data using Merkle tree-based mechanisms, preventing tampering or unauthorized alterations.
2. *Resilience to Cryptographic Attacks*:
   - The proposed framework demonstrates resilience against a variety of cryptographic attacks, such as:
     - Impersonation attacks.
     - Offline password guessing attacks.
     - Key-Stroke Session Timeout Identity Attack (KSSTIA).
3. *Enhanced Authentication*:
   - A robust three-factor privacy-preserving authentication mechanism is implemented, providing:
     - Mutual authentication between users and servers.
     - Session key security to protect ongoing communication.

2. Privacy Preservation

1. *User Anonymity*:
   - The system ensures that user identities remain anonymous during data interactions, thus preventing unauthorized tracing of users.
2. *Certificate-less Authentication*:

- By adopting certificateless cryptography, the protocol eliminates the overhead of traditional Public Key Infrastructure (PKI) while ensuring privacy and secure key management.

3. Computational and Communication Efficiency

1. *Use of Elliptic Curve Cryptography (ECC)*:
   - ECC significantly enhances computational efficiency with smaller key sizes, making the protocol suitable for resource-constrained environments like IoT devices in DT setups.
2. *Optimized Protocol*:
   - Compared to existing solutions, the proposed protocol achieves:
     - Reduced computational costs.
     - Comparable communication costs.
     - Superior security measures.

4. Scalability and Flexibility

1. *Scalability for IoT Applications*:
   - The protocol supports large-scale DT environments, accommodating numerous IoT devices without degrading performance.
2. *Decentralized Verification*:
   - Blockchain enables decentralized transaction verification, reducing reliance on a central authority and enhancing scalability.

5. Real-World Applicability

1. *Domain-Specific Benefits*:
   - The framework is particularly beneficial for:
     - Healthcare: Ensuring privacy-preserving real-time monitoring and secure data sharing.
     - Autonomous Vehicles: Secure and real-time data exchange for traffic control and navigation.
     - Smart Cities: Efficient and secure data integration for urban planning and management.
2. *Support for Cloud-Assisted DT*:
   - By leveraging cloud computing, the protocol facilitates real-time data processing, simulation, and analysis in DT environments.

6. Future-Proof Security Enhancements

1. *Foundations for Quantum-Resistant Protocols*:
   - The design sets the stage for incorporating quantum-resistant cryptographic algorithms, addressing future computational threats.
2. *Dynamic Security Adjustments*:
   - The framework's modular design allows for the integration of advanced anomaly detection and policy management mechanisms.

7. Testing and Validation Outcomes

1. *Security Analysis*:
   - Informal security analysis confirms that the protocol effectively mitigates several security threats.
   - Formal validation using the ROR (Real-Or-Random) Model and BAN logic ensures mutual authentication and session key security.
2. *Robust Performance in Simulated Environments*:
   - Testing demonstrated seamless performance across various scenarios, ensuring that the protocol meets practical and theoretical security benchmarks.

8. Impact on Existing Research and Applications

1. *Addressing Gaps in Prior Work*:
   - The report identifies limitations in existing protocols (e.g., lack of user anonymity, susceptibility to impersonation) and overcomes them with a more resilient framework.
2. *Practical Contributions*:
   - Provides a concrete solution for real-world challenges in deploying secure DT environments, thus paving the way for future innovations.

The proposed privacy-preserving blockchain-assisted protocol effectively balances the demands of security, efficiency, and scalability in DT environments. It provides a robust foundation for addressing existing vulnerabilities in IoT and cloud-based systems, while also ensuring adaptability for future technological advancements. This framework establishes a benchmark for secure and efficient communication in next-generation DT ecosystems.

CONCLUSION.

Examined various design flaws and vulnerabilities in opposition to numerous cryptographic attacks, like user impersonation, KSSTIA, and offline password guessing attacks. By utilizing block chain technology, we proposed an enhanced three-factor-based privacy-preserving authentication framework for the DT environment. The informal security analysis of the proposed scheme shows the efficiency and enhanced security against various wicked attacks. The mutual authentication and session key security is also ensured by performing the formal analysis of the proposed work using both the ROR Model and BAN logic. Moreover, compared to the competing existing works, the proposed method offers reduced computation costs, comparable communication costs, and superior security. Therefore, the proposed work is suitable for the DT environment. In future, we would like enhance the proposed scheme with more efficiency in terms of communication, computational and storage costs while keeping the same security level. In addition, we would also like to develop a complete test bed experiment for practical aspects of the proposed scheme.

Scope for future enhancement.

- Integration of advanced AI-driven anomaly detection to identify and mitigate potential security threats in real-time.
- Incorporation of quantum-resistant cryptographic algorithms to future-proof the system against emerging quantum computing threats.
- Enhancement of scalability to support even larger and more complex Digital Twin environments, including global networks of IoT devices.
- Development of a cross-chain interoperability feature to enable integration with other blockchain networks and systems.
- Implementation of dynamic policy management to adjust security and privacy measures based on contextual factors and user requirements.
- Introduction of user-centric privacy controls, allowing individuals to have more granular control over their data and its usage.

REFERENCES :

[1] M. Grieves and J. Vickers, ‘‘Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems,’’ in *Transdisciplinary Perspectives on Complex Systems: New Findings and Approaches*. Cham, Switzerland: Springer, 2017, pp. 85–113.

[2] B. Piascik, J. Vickers, D. Lowry, S. Scotti, J. Stewart, and A. Calomino,‘‘Materials, structures, mechanical systems, and manufacturing roadmap,’’ NASA, Washington, DC, USA, Tech. Rep. TA 12, 2012.

[3] H. Laaki, Y. Miche, and K. Tammi, ‘‘Prototyping a digital twin for real time remote control over mobile networks: Application of remote surgery,’’ *IEEE Access*, vol. 7, pp. 20325–20336, 2019.

[4] H. Wang and J. Zhang, ‘‘Blockchain based data integrity verification for large-scale IoT data,’’ *IEEE Access*, vol. 7, pp. 164996–165006,2019.

[5] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, ‘‘Blockchain data-based cloud data integrity protection mechanism,’’ *Future Gener. Comput. Syst.*, vol. 102, pp. 902–911, Jan. 2020.

[6] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, ‘‘Blockchain based data integrity service framework for IoT data,’’ in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jun. 2017, pp. 468–475.

[7] S. Son, D. Kwon, J. Lee, S. Yu, N.-S. Jho, and Y. Park, ‘‘On the design of a privacy-preserving communication scheme for cloud-based digital twin environments using blockchain,’’ *IEEE Access*, vol. 10, pp. 75365–75375, 2022.

[8] T.-Y. Wu, Y.-Q. Lee, C.-M. Chen, Y. Tian, and N. A. Al-Nabhan, ‘‘An enhanced pairing-based authentication scheme for smart grid communications,’’ *J. Ambient Intell. Humanized Comput.*, vol. 2021, pp. 1–13, Jan. 2021.

[9] S. Khatoon, S. M. M. Rahman, M. Alrubaian, and A. Alamri, ‘‘Privacy preserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment,’’ *IEEE Access*, vol. 7, pp. 47962–47971, 2019.

[10] A. Sengupta, A. Singh, P. Kumar, and T. Dhar, ‘‘A secure and improved two factor authentication scheme using elliptic curve and bilinear pairing for cyber physical systems,’’ *Multimedia Tools Appl.*, vol. 16, pp. 1–24, Jul. 2022.

[11] H. S. Grover and D. Kumar, ‘‘Cryptanalysis and improvement of a three factor user authentication scheme for smart grid environment,’’ *J. Reliable Intell. Environ.*, vol. 6, no. 4, pp. 249–260, Dec. 2020.

[12] M.Wazid, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, ‘‘Secure three factor user authentication scheme for renewable-energy-based smart grid environment,’’ *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3144–3153,Dec. 2017.

[13] D. Kaur and D. Kumar, ‘‘Cryptanalysis and improvement of a two-factor user authentication scheme for smart home,’’ *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102787.

[14] M. Shuai, N. Yu, H. Wang, and L. Xiong, ‘‘Anonymous authentication scheme for smart home environment with provable security,’’ *Comput.Secur.*, vol. 86, pp. 132–146, Sep. 2019.

[15] Y. Chen, J. Martinez, P. Castillejo, and L. López, ‘‘A bilinear map pairing based authentication scheme for smart grid communications: PAuth,’’ *IEEE Access*, vol. 7, pp. 22633–22643, 2019.

[16] M. Nikooghadam and H. Amintoosi, ‘‘Cryptanalysis of Khatoon et al.’s ECC-based authentication protocol for healthcare systems,’’ 2019, *arXiv:1906.08424*.

[17] M. Abdalla, P.-A. Fouque, and D. Pointcheval, ‘‘Password-based authenticated key exchange in the three-party setting,’’ in *Proc. Int.Workshop Public Key Cryptogr.* Cham, Switzerland: Springer, 2005, pp. 65–84.

[18] M. Burrows, M. Abadi, and R. Needham, ‘‘A logic of authentication,’’ *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, Feb. 1990.

[19] A. K. Das and B. Bruhadeshwar, ‘‘An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system,’’ *J. Med. Syst.* vol. 37, no. 5, p. 9969, 2013.

[20] S. Chatterjee and A. K. Das, ‘‘An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks,’’ *Secur. Commun. Netw.*, vol. 8, no. 9, pp. 1752–1771, 2015.